UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,030	03/26/2004	Jan Hofmeyr	MS1-2018US	9067

22801 7590 09/11/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,030	HOFMEYR ET AL.	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-40 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 22-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 22-34 are drawn to a computer-readable medium that is described in the specification as being a communication medium such as a carrier wave or other transport mechanism (see Page 21, paragraph 72 and Page 22, paragraph 75). Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in §101 (Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf, 1300 OG 142 (Nov. 22, 2005)).

3. The Supreme Court has read the term "manufacture" in accordance with its dictionary definition to mean "the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery." Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980) (quoting American Fruit Growers, Inc. v Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See

American Disappearing Bed Co. v. Arnaelsteen, 182 F.324, 325 (9th Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statue without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act.

4. A manufacture is also defined as the residual class of product. 1 Chisum, §1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two products classes, machine and composition of matter, require physical matter. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of §101.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 16 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for "the encryption method packet is delivered via a private table," does not reasonably provide enablement for "inserting the multiplex-compliant encryption method packet into the transport stream," and "the encryption method packet is delivered via a private table." The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these

claims. The specification specifies that the encryption method packet is inserted into the transport stream **OR** delivered via a private table (See Page 17, paragraph 57).

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 15, 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 15 recites, "a location of the encrypted portion of the unencrypted portion of the transport stream," which renders the claim indefinite because an unencrypted portion of a transport stream cannot include an encrypted portion.

10. Claim 39 recites the limitation "the analysis" in line 6. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1-15, 17-26, 28-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Candelore, U.S. Patent No. 7,124,303. Referring to claim 1, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams

to determine which packets should be encrypted (Col. 13, lines 27-33), which meets the limitation of analyzing a transport stream. The transport streams are encrypted such that new or non-legacy settop boxes receive the encrypted streams and determine how the packets are encrypted (Col. 13, lines 18-25, 62-66). If a packet is encrypted under system A, the packet is discarded or ignored (Col. 13, lines 21-22, 65-66), which meets the limitation of preparing the transport stream for processing that bypasses encrypted portions of the transport stream.

Referring to claim 2, Candelore discloses that if it is determined by the headend that a packet need not be encrypted, it is directly inserted into the output stream (Col. 13, lines 31-35), which meets the limitation of analyzing the transport stream includes determining which portions of the transport stream are to pass unencrypted.

Referring to claims 3, 4, Candelore discloses that the determination of which packets are encrypted can be made based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14), which meets the limitation of determining which portions of the transport stream are to pass unencrypted is executed based on a statistical analysis, dynamically.

Referring to claims 5, 7, Candelore discloses that the cable headend may encrypt only transport stream packets containing PES headers and other headers as part of the payload, since without this information, the settop box decoder cannot decompress the MPEG compressed data (Col. 18, lines 55-64), which meets the limitation of determining which portions of the transport stream are to pass unencrypted includes determining a permissible incursion beyond a packet header to gather data for the processing, detecting bytes of data that are required for processing the transport stream.

Referring to claim 6, Candelore discloses that the cable headend may encrypt only transport stream packets containing PES headers (Col. 18, lines 55-66), which meets the limitation of determining which portions of the transport stream are to pass unencrypted includes detecting a data packet containing at least a portion of a packetized elementary stream (PES) header.

Referring to claim 8, Candelore discloses that the cable headend determine that certain packets should be encrypted (Col. 13, lines 35-44 & Col. 18, lines 55-64), which meets the limitation of preparing the transport stream for processing includes encrypting portions of the transport stream that are not to pass unencrypted.

Referring to claims 9, 12, Candelore discloses that the cable headend may encrypt only transport stream packets containing PES headers and other headers as part of the payload (Col. 18, liens 55-64), which meets the limitation of preparing the transport stream for processing includes encrypting packets containing PES payload data, common scrambling packets composed of PES payload data.

Referring to claims 10, 11, Candelore discloses that the cable headend may encrypt only audio portions of the transport stream while leaving the video portions unencrypted (Col. 6, lines 25-46), which meets the limitation of preparing the transport stream for processing includes leaving a packet containing a portion of a frame header unencrypted, preparing the transport stream for processing includes leaving bytes of data unencrypted that are required for processing the transport stream.

Referring to claim 13, Candelore discloses creating a program specific information data stream that is multiplexed with the transport stream packets (Col. 11, lines 45-50), which meets

the limitation of generating a multiplex-compliant encryption method packet, and inserting the multiplex-compliant encryption method packet into the transport stream.

Referring to claim 14, Candelore discloses that the program specific information includes ECMs that are used to get descrambling keys (Col. 7, lines 17-19 & Col. 8, lines 38-36), which meets the limitation of the encryption method packet provides data for deriving a decryption key. The CA descriptors included in the program specific information identifies encrypted portions of the transport stream (Col. 12, lines 22-23), which meets the limitation of identifies encrypted portions of the transport stream. Table 1 shows that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of identifies an encryption algorithm used in preparing the transport stream for processing.

Referring to claim 15, to the extent understood, Candelore discloses in Table 1 that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of the encryption method packet identifies a unencrypted portion of the transport stream, a location of the encrypted portion of the unencrypted portion of the transport stream, and a process corresponding to the unencrypted portion of the transport stream.

Referring to claim 17, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33), which meets the limitation of receiving a partially encrypted transport stream. The transport streams are encrypted such that new or non-legacy

settop boxes receive the encrypted streams and determine how the packets are encrypted (Col. 13, lines 18-25, 62-66). If a packet is encrypted under system A, the packet is discarded or ignored (Col. 13, lines 21-22, 65-66), which meets the limitation of processing the transport stream in a manner that bypasses encrypted portions of the transport stream.

Referring to claim 18, Candelore discloses creating a program specific information data stream that is multiplexed with the transport stream packets (Col. 11, lines 45-50), which meets the limitation of receiving a multiplex-compliant encryption method packet corresponding to the transport stream. The program specific information includes ECMs that are used to get descrambling keys (Col. 7, lines 17-19 & Col. 8, lines 38-36), which meets the limitation of decrypting encrypted portions of the transport stream using a decryption key.

Referring to claim 19, Candelore discloses that the program specific information includes ECMs that are used to get descrambling keys (Col. 7, lines 17-19 & Col. 8, lines 38-36), which meets the limitation of the decryption key is included in the encryption method packet.

Referring to claim 20, Candelore discloses that the unencrypted packets and the encrypted packets are multiplexed into a single stream that is transmitted to the settop boxes such that the unencrypted packets are output for display and the encrypted packets are decrypted prior to being output (Col. 6, lines 43-54), which meets the limitation of processing the transport stream includes demultiplexing the transport stream based on unencrypted portions of the transport stream.

Referring to claim 21, Candelore discloses in Table 1 that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets

the limitation of processing the transport stream includes indexing payload data contained in the transport stream based on unencrypted portions of the transport stream.

Referring to claim 22, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33). It is determined by the headend that a packet need not be encrypted, it is directly inserted into the output stream (Col. 13, lines 31-35), which meets the limitation of determine which portions of a transport stream are to pass unencrypted, prepare the transport stream for the processing. The transport streams are encrypted such that new or non-legacy settop boxes receive the encrypted streams and determine how the packets are encrypted (Col. 13, lines 18-25, 62-66). If a packet is encrypted under system A, the packet is discarded or ignored (Col. 13, lines 21-22, 65-66), which meets the limitation of processing that disregards encrypted portions of the transport stream.

Referring to claims 23, 24, Candelore discloses that the cable headend may encrypt only audio portions of the transport stream while leaving the video portions unencrypted (Col. 6, lines 25-46), which meets the limitation of the one or more instructions to determine which portions of the transport stream are to pass unencrypted cause the one or more processors to leave unencrypted data packets having at least a portion of a PES header, and leave unencrypted bytes of data required for processing the transport stream.

Referring to claim 25, Candelore discloses that the determination of which packets are encrypted can be made based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14), which meets the limitation of the one or more instructions to determine which portions of the transport stream are to pass unencrypted cause the one or more

processors to leave unencrypted a threshold amount of data beyond packet header data that is relevant for the processing.

Referring to claim 26, Candelore discloses that the cable headend determine that certain packets should be encrypted (Col. 13, lines 35-44 & Col. 18, lines 55-64), which meets the limitation of the one or more instructions to prepare the transport stream for processing cause the one or more processors to encrypt portions of the transport stream that are not to pass unencrypted.

Referring to claim 28, Candelore discloses creating a program specific information data stream that is multiplexed with the transport stream packets (Col. 11, lines 45-50), which meets the limitation of generating a multiplex-compliant encryption method packet, and inserting the multiplex-compliant encryption method packet into the transport stream.

Referring to claim 29, Candelore discloses that the program specific information includes ECMs that are used to get descrambling keys (Col. 7, lines 17-19 & Col. 8, lines 38-36), which meets the limitation of the encryption method packet provides data for deriving a decryption key. The CA descriptors included in the program specific information identifies encrypted portions of the transport stream (Col. 12, lines 22-23), which meets the limitation of identifies encrypted portions of the transport stream. Table 1 shows that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of identifies an encryption algorithm used in preparing the transport stream for processing.

Referring to claim 30, Candelore discloses in Table 1 that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for

not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of the encryption method packet identifies a unencrypted portion of the transport stream, a location of the unencrypted portion of the transport stream, and a process corresponding to the unencrypted portion of the transport stream.

Referring to claim 31, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33), which meets the limitation of receive a partially encrypted transport stream. Table 1 shows that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of process the transport stream based on unencrypted portions of the transport stream.

Referring to claim 32, Candelore discloses creating a program specific information data stream that is multiplexed with the transport stream packets (Col. 11, lines 45-50), which meets the limitation of receive a multiplex-compliant encryption method packet corresponding to the transport stream. The program specific information includes ECMs that are used to get descrambling keys (Col. 7, lines 17-19 & Col. 8, lines 38-36), which meets the limitation of decrypt encrypted portions of the transport stream using a decryption key based in the encryption method packet.

Referring to claim 33, Candelore discloses that the unencrypted packets and the encrypted packets are multiplexed into a single stream that is transmitted to the settop boxes such that the unencrypted packets are output for display and the encrypted packets are decrypted prior to being output (Col. 6, lines 43-54), which meets the limitation of the one or more instructions

to process the transport stream cause the one or more processors to demultiplex the transport stream based on unencrypted portions of the transport stream.

Referring to claim 34, Candelore discloses in Table 1 that each packet has an identifier that indicates the type of encryption used on the packet (Col. 11-12, table 1, showing 'clear' for not encrypted, 'EA' for encryption process A, and 'EB' for encryption process B), which meets the limitation of the one or more instructions to process the transport stream cause the one or more processors to index payload data contained in the transport stream based on unencrypted portions of the transport stream.

Referring to claim 35, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33). If it is determined by the headend that a packet need not be encrypted, it is directly inserted into the output stream (Col. 13, lines 31-35), which meets the limitation of an analyzer to determine which portions of a transport stream are to pass unencrypted for processing. If the packet is to be encrypted, the packet is encrypted based on different encryption processes before being inserted into the output stream (Col. 13, lines 35-44), which meets the limitation of a scrambler to encrypt other portions of the transport stream based on the determination. The transport streams are encrypted such that new or non-legacy settop boxes receive the encrypted streams and determine how the packets are encrypted (Col. 13, lines 18-25, 62-66). If a packet is encrypted under system A, the packet is discarded or ignored (Col. 13, lines 21-22, 65-66), which meets the limitation of processing that does not incorporate encrypted portions of the transport stream.

Referring to claim 36, Candelore discloses that the cable headend may encrypt only transport stream packets containing PES headers and other headers as part of the payload, since without this information, the settop box decoder cannot decompress the MPEG compressed data (Col. 18, lines 55-64), which meets the limitation of the analyzer is to dynamically determine that a threshold incursion into payload data is to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.

Referring to claims 37, 38, Candelore discloses that the cable headend may encrypt only audio portions of the transport stream while leaving the video portions unencrypted (Col. 6, lines 25-46), which meets the limitation of the analyzer is to determine that a packet containing at least a portion of a PES header is to pass unencrypted, determine that data arbitrarily disposed throughout PES payload data are to pass unencrypted.

Referring to claim 39, Candelore discloses a partial encryption system for transport streams wherein the cable system headend analyzes the streams to determine which packets should be encrypted (Col. 13, lines 27-33). If it is determined by the headend that a packet need not be encrypted, it is directly inserted into the output stream (Col. 13, lines 31-35), which meets the limitation of means for determining which portions of a transport stream are to pass unencrypted for processing. If the packet is to be encrypted, the packet is encrypted based on different encryption processes before being inserted into the output stream (Col. 13, lines 35-44), which meets the limitation of means for encrypting other portions of the transport stream in accordance with the analysis. The transport streams are encrypted such that new or non-legacy settop boxes receive the encrypted streams and determine how the packets are encrypted (Col. 13, lines 18-25, 62-66). If a packet is encrypted under system A, the packet is discarded or

ignored (Col. 13, lines 21-22, 65-66), which meets the limitation of processing that does not incorporate encrypted portions of the transport stream.

Referring to claim 40, Candelore discloses that the determination of which packets are encrypted can be made based upon a desired balance of bandwidth usage and security against hackers (Col. 10, lines 11-14), which meets the limitation of means for determining designates a dynamically determined amount of payload data to pass unencrypted in order to process the transport stream without removing the encryption from other portions of the transport stream.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

15. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore, U.S. Patent No. 7,124,303, in view of Lyle, U.S. Patent No. 7,242,766. Referring to claim 27, Candelore does not specify using the CTR mode of AES encryption in the partial encryption system for transport streams. However, it would have been obvious to one of ordinary skill in the

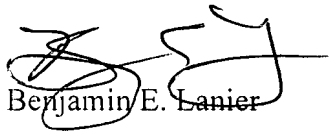
art at the time the invention was made to use the CTR mode of AES encryption in the partial encryption system of Candelore because the CTR mode of AES encryption provides reduced computational requirements when operating at high speeds while retaining some of the security benefits as taught by Lyle (Col. 15, lines 3-29).

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier